**UNITED STATES DISTRICT COURT**
**DISTRICT OF NEBRASKA**

| | |
|---|---|
| **In Re Signature Performance Data Breach Litigation** | **Case No. 8:24CV230**<br><br>**DEMAND FOR A JURY TRIAL** |

# CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Curtis Mclean, Brandi Canady, Rachael Reese, Lea Jacobs, Eloyd Long, Monica Enriquez, David Underwood, and Orneze Coit (collectively "Plaintiffs"), on behalf of themselves and all others similarly situated persons, allege the following against Signature Performance, Inc. ("Signature"), Southeastern Regional Medical Center d/b/a UNC Health Southeastern ("UNC Health"), and Adventist Health System/West and Adventist Health Tulare (collectively, "Adventist") (all collectively, "Defendants"). Plaintiffs allege the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to each Plaintiff, which are alleged upon their personal knowledge.

## I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated patients' personally identifiable information ("PII") and protected health information ("PHI"), including names, addresses, phone numbers, dates of birth, Social Security numbers, provider names, dates of services, medical record/case numbers, Medicare/Medicaid ID numbers, health insurance provider names, health insurance individual policy numbers, and/or treatment costs (the "Private Information"), from criminal hackers.

2. Defendant Signature, based in Omaha, Nebraska, is a healthcare administration and solutions provider that serves more than 40 medical facilities across the United States.

3. Defendant UNC Health provides health care services to patients in North Carolina, and Adventist provides health care services to patients in California, including at Adventist Health Tulare.

4. On or about February 9, 2024, Signature filed official notice of a hacking incident with the Maine Attorney General's Office. Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

5. On or about June 10, 2024, Signature also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the Data Breach.

6. Based on the Notice sent to Plaintiffs and "Class Members" (defined below), unusual activity was detected on some of Signature's computer systems. In response, Defendant Signature initiated an investigation which revealed that an unauthorized party had access to certain files that contained sensitive patient information maintained by Defendants, and that such access took place between January 17 and January 18, 2024 (the "Data Breach"). Yet, Defendants waited five months to notify the public that they were at risk.

7. As a result of this delayed response, Plaintiffs and Class Members had no idea for five months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, Social Security numbers, provider names, dates of services, medical record/case

numbers, Medicare/Medicaid ID numbers, health insurance provider names, health insurance individual policy numbers, and/or treatment costs that Defendants collected and maintained.

9. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. There has been no assurance offered by Defendants that all personal data or copies of data have been recovered or destroyed, or that Defendants have adequately enhanced their data security practices sufficient to avoid a similar breach of their network in the future.

11. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

12. Plaintiffs bring this class action lawsuit to address Defendants' inadequate safeguarding of Class Members' Private Information that Defendants collected and maintained, and their failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

13. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

14. Upon information and belief, Defendants failed to properly implement security practices with regard to the computer network and systems that housed the Private Information. Had Defendants properly monitored their networks, the Defendants would have discovered the Breach sooner.

15. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct as the Private Information that Defendants collected and maintained is now in the hands of data thieves and other unauthorized third parties.

16. Plaintiffs seek to remedy these harms on behalf of themselves individually and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, breach of implied contract, invasion of privacy, unjust enrichment, breach of fiduciary duty, breach of third-party beneficiary contract, violation of the California Consumer Privacy Act, violation of California Business & Professions Code § 17200, *et seq*., violation of the California Customer Records Act, violation of the California Confidentiality of Medical Information Act, declaratory judgment, and all other relief that this Court deems just and proper.

## II. PARTIES

***Plaintiffs***

17. Plaintiff Curtis Mclean is a natural person, resident, and a citizen of the state of North Carolina. Plaintiff has no intention of moving to a different state in the immediate future.

Plaintiff brings this case on his own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff's Private Information and owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Mclean would not have entrusted his Private Information to Defendants had he known that Defendants failed to maintain adequate data security. Plaintiff received a notice letter indicating that his Private Information was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

18. Plaintiff Brandi Canady is a natural person, resident, and a citizen of the state of North Carolina. Plaintiff has no intention of moving to a different state in the immediate future. Plaintiff brings this case on her own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff's Private Information and owed her a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Canady would not have entrusted her Private Information to Defendants had she known that Defendants failed to maintain adequate data security. Plaintiff received a notice letter indicating that her Private Information was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

19. Plaintiff Rachael Reese is a natural person, resident, and a citizen of the state of California. Plaintiff has no intention of moving to a different state in the immediate future. Plaintiff brings this case on her own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff's Private Information and owed her a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Reese would not have entrusted her Private Information to Defendants had she known that Defendants failed to maintain adequate data security. Plaintiff received a notice letter indicating that her Private

Information was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

20. Plaintiff Lea Jacobs is a natural person, resident, and a citizen of the state of North Carolina. Plaintiff has no intention of moving to a different state in the immediate future. Plaintiff brings this case on her own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff's Private Information and owed her a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Jacobs would not have entrusted her Private Information to Defendants had she known that Defendants failed to maintain adequate data security. Plaintiff received a notice letter indicating that her Private Information was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

21. Plaintiff Eloyd Long is a natural person, resident, and a citizen of the state of California. Plaintiff has no intention of moving to a different state in the immediate future. Plaintiff brings this case on his own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff's Private Information and owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Long would not have entrusted his Private Information to Defendants had he known that Defendants failed to maintain adequate data security. Plaintiff received a notice letter indicating that his Private Information was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

22. Plaintiff Monica Enriquez is a natural person, resident, and a citizen of the state of California. Plaintiff has no intention of moving to a different state in the immediate future. Plaintiff brings this case on her own behalf and on behalf of others similarly situated. Defendants obtained

and continue to maintain Plaintiff's Private Information and owed her a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Enriquez would not have entrusted her Private Information to Defendants had she known that Defendants failed to maintain adequate data security. Plaintiff received a notice letter indicating that her Private Information was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

23. Plaintiff David Underwood is a natural person, resident, and a citizen of the state of California. Plaintiff has no intention of moving to a different state in the immediate future. Plaintiff brings this case on her own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff's Private Information and owed her a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Underwood would not have entrusted his Private Information to Defendants had he known that Defendants failed to maintain adequate data security. Plaintiff received a notice letter indicating that his Private Information was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

24. Plaintiff Orneze Coit is a natural person, resident, and a citizen of the state of Georgia. Plaintiff has no intention of moving to a different state in the immediate future. Plaintiff brings this case on his own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff's Private Information and owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Coit would not have entrusted his Private Information to Defendants had he known that Defendants failed to maintain adequate data security. Plaintiff received a notice letter indicating that his Private

Information was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

***Defendants***

25. Defendant Signature Performance, Inc. is a Nebraska corporation with its principal place of business at 10250 Regency Circle, Suite 500 Omaha, NE 68114-3736. Defendant is a provider of healthcare administrative solutions and services.

26. Defendant Southeastern Regional Medical Center d/b/a UNC Health Southeastern is a North Carolina corporation with its principal place of business at 300 W 27th St, Lumberton, NC 28358.

27. Defendant Adventist Health System/West is a California corporation with its principal place of business at 1 Adventist Health Way, Roseville, CA 95661.

28. Defendant Adventist Health Tulare is a California corporation with its principal place of business at 869 N. Cherry St., Tulare, CA 93274.

## III. JURISDICTION AND VENUE

29. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

30. This Court has general personal jurisdiction over Signature because it is a Nebraska corporation that operates and has its principal place of business in this District.

31. This Court has specific personal jurisdiction over Defendants UNC Health and Adventist because they purposely availed themselves of Nebraska in using Signature as an administrative services provider.

32. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant Signature is domiciled in this District and maintains Plaintiffs' and Class Members' Private Information in this District.

## IV. FACTUAL ALLEGATIONS

### *A. Defendants' Business and Collection of Plaintiffs' and Class Members' Private Information.*

33. At all relevant times, Defendants knew they were storing sensitive Private Information and that, as a result, Defendants' systems would be attractive targets for cybercriminals.

34. Defendants also knew that any breach of their systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

35. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at major businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

36. As a condition of receiving healthcare services, Defendants require that patients entrust them with highly sensitive personal and health information. In the ordinary course of receiving service from Defendants, Plaintiffs and Class Members were required to provide their Private Information to Defendants.

37. Upon information and belief, Defendants made promises and representations to consumers, including Plaintiffs and Class Members, that the Private Information collected from them would be kept safe, confidential, and that the privacy of that information would be maintained.

38. As a result of collecting and storing the Private Information of Plaintiffs and Class Members for their own financial benefit, Defendants had a continuous duty to adopt and employ reasonable measures to protect Plaintiffs' and the Class Members' Private Information from disclosure to third parties.

39. In its Notice of Privacy Practices, Defendant Signature promises its patients that it is "committed to the privacy of your health information" and says that it is required by law to "use strict privacy standards to protect your health information from unauthorized use or disclosure."[1] Signature also describes in its Privacy Policy the limited specific instances when it shares patient health information.[2]

40. Thus, due to the highly sensitive and personal nature of the information Defendants acquire and store with respect to their patients, Defendants, upon information and belief, promise to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of patients' Private Information; inform patients of their legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

[1] *See* https://www.signatureperformance.com/privacypolicy.
[2] *Id.*

41. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties they owed to them and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

42. Plaintiffs and Class Members relied on Defendants to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendants ultimately failed to do.

***B. The Data Breach and Defendants' Inadequate Notice to Plaintiffs and Class Members.***

43. According to Defendant Signature's Notice, it learned of unauthorized access to its computer systems on January 18, 2024, with such unauthorized access having taken place between January 17 and January 18, 2024.

44. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including name, address, phone number, date of birth, Social Security number, provider name, dates of service, medical record/case number, Medicare/Medicaid ID number, health insurance provider name, health insurance individual policy number, and/or treatment cost.

45. On or about June 10, 2024, roughly five months after Defendants learned that the Class's Private Information was first accessed by cybercriminals, Signature, on behalf of all the Defendants, finally began to notify patients that their investigation determined that their Private Information was impacted.

46. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

47. Plaintiffs and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such Private Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

48. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks in the health care industry in recent years.

49. Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

### *C. The Healthcare Sector Is Particularly Susceptible to Data Breaches.*

50. At all relevant times, Defendants, as healthcare companies, knew they were storing sensitive Private Information and that, as a result, Defendants' systems would be attractive targets for cybercriminals.

51. Defendants also knew that any breach of their systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

52. Defendants were also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related

systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[3]

53. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[4]

54. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[5] In 2022, the largest growth in compromises occurred in the healthcare sector.[6]

55. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[7]

---

[3] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on August 19, 2024).

[4] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on August 19, 2024).

[5]Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on August 19, 2024).

[6]Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on August 19, 2024).

[7] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on August 19, 2024).

56. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[8]

57. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[9]

58. Due to the high-profile nature of these breaches and other breaches of its kind, Defendants were and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack.

59. As healthcare companies, Defendants knew, or should have known, the importance of safeguarding their patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Defendants' patients as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

---

[8] *Id*.

[9] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on August 19, 2024).

***D. Defendants Failed to Comply with HIPAA.***

60. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendants left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

61. Defendants' Data Breach resulted from a combination of insufficiencies that indicate Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Defendants' Data Breach that Defendants either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

62. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

63. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

64. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

65. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

66. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

67. Based upon Defendants' Notice to Plaintiffs and Class Members, Defendants reasonably believe that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

68. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

69. Plaintiffs reasonably believe that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

70. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

71. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

72. Defendants reasonably believe that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

73. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as

a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

74. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

75. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

76. In addition, Defendants' Data Breach could have been prevented if Defendants had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored their obligations to their patients.

77. Defendants' security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only

to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

78. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

79. Because Defendants failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Defendants' approach to information security is adequate and appropriate going forward. Defendants still maintain the PHI and other highly sensitive PII of their current and former patients, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

### *E. Defendants Failed to Comply with FTC Guidelines.*

80. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

81. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating

someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

82. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

83. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

85. Defendants were at all times fully aware of their obligation to protect the Private Information of patients yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

### *F. Defendants Failed to Comply with Industry Standards.*

86. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

87. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like the Defendants do, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

88. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

89. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

90. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

### *G. Defendants Breached their Duty to Safeguard Plaintiffs' and Class Members' Private Information.*

91. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing,

safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the Private Information of Class Members

92. Defendants breached their obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to sufficiently train their employees regarding the proper handling of their patients Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

93. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access their computer network and systems which contained unsecured and unencrypted Private Information.

94. Had Defendants remedied the deficiencies in their information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

95. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendants.

### *H. Defendants Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft.*

96. The FTC hosted a workshop to discuss "informational injuries," which are injuries that patients like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[10] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment.

97. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity

[10] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on August 19, 2024)

thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

98. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

99. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

100. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

101. One such example of this is the development of "Fullz" packages.

102. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally

stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

103. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

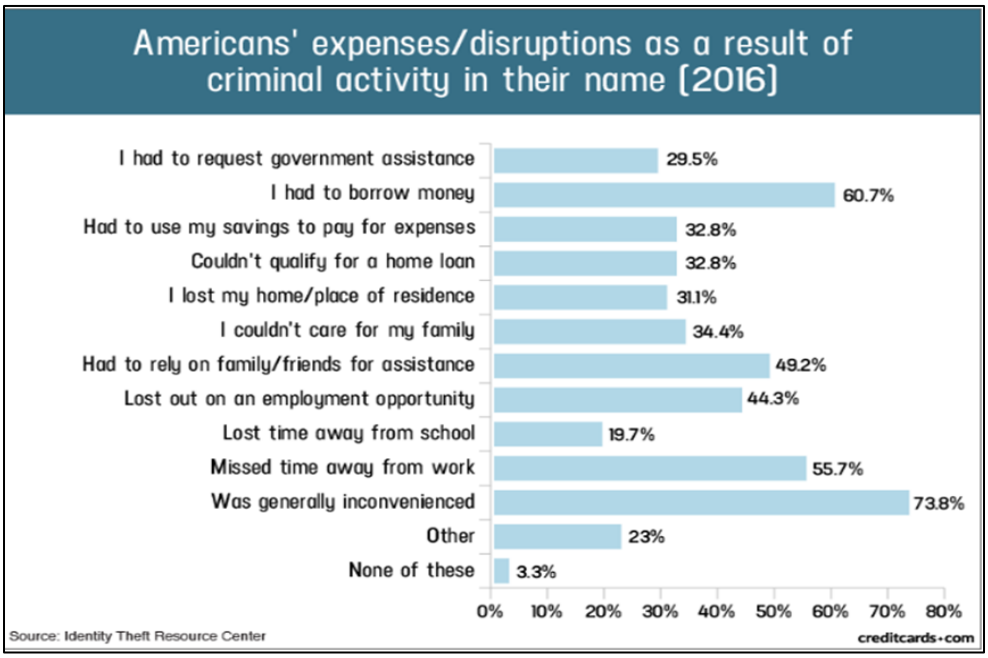
104. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[11] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

105. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the

[11] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited August 19, 2024).

thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

106. In fact, a study by the Identity Theft Resource Center[12] shows the multitude of harms caused by fraudulent use of PII:




107. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[13]

[12] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on August 19, 2024)

[13] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on August 19, 2024).

108. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

109. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[14]

110. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

111. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[15]

112. The ramifications of Defendants' failure to keep their patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

[14]Center for Internet Security, *Data Breaches: In the Healthcare Sector*, *available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on August 19, 2024).

[15] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on August 19, 2024).

113. Here, not only was sensitive medical information compromised, but financial information and Social Security numbers were compromised too. The value of Private Information is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

114. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[16]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

115. Private Information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

116. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for their lifetimes.

## *I. Plaintiffs' and Class Members' Damages*

**Plaintiff Curtis Mclean's Experience**

[16] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited August 19, 2024)

117. Plaintiff McLean is a former patient of UNC Health Southeastern.

118. As a condition of obtaining healthcare services, Plaintiff McLean was required to provide his Private Information to Defendants, including his name, address, date of birth, Social Security number, phone number, and insurance identification number, among other sensitive information.

119. At the time of the Data Breach, Defendants maintained Plaintiff McLean's Private Information in their system.

120. Plaintiff McLean is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff McLean would not have entrusted his Private Information to Defendants had he known of Defendants' lax data security policies.

121. Plaintiff McLean received the Notice Letter, by U.S. mail, directly from Defendant Signature, on June 10, 2024. According to the Notice Letter, Plaintiffs' Private Information was improperly accessed and obtained by unauthorized third parties, including his address, phone number, date of birth, Social Security number, provider name, dates of service, medical record/case number, Medicare/Medicaid ID number, health insurance provider name, health insurance individual policy number, and/or treatment cost.

122. As a result of the Data Breach, Plaintiff McLean made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff McLean has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

123. Plaintiff McLean suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

124. Plaintiff McLean additionally suffered actual injury in the form of two unauthorized credit cards being opened under his name in mid-April 2024 which were identified on his credit report.

125. Plaintiff McLean additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

126. The Data Breach has caused Plaintiff McLean to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence. Specifically, Plaintiff McLean is unable to sleep well as a result of the recent misuse of his compromised Private Information resulting from the Data Breach.

127. As a result of the Data Breach, Plaintiff McLean anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

128. As a result of the Data Breach, Plaintiff McLean is at a present risk and will continue to be at increased risk of identity theft and fraud for his lifetime.

129. Plaintiff McLean has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

**Plaintiff Brandi Canady's Experience**

130. Plaintiff Canady is a patient at UNC Health Southeastern.

131. As a condition of obtaining healthcare services, Plaintiff Canady was required to provide her Private Information to Defendants, including her name, address, date of birth, Social Security number, phone number, and insurance identification number, among other sensitive information.

132. At the time of the Data Breach, Defendants maintained Plaintiff Canady's Private Information in their system.

133. Plaintiff Canady is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location.

She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Canady would not have entrusted her Private Information to Defendants had she known of Defendants' lax data security policies.

134. Plaintiff Canady received the Notice Letter, by U.S. mail, directly from Defendant Signature, on June 10, 2024. According to the Notice Letter, Plaintiff Canady's Private Information was improperly accessed and obtained by unauthorized third parties, including her address, phone number, date of birth, Social Security number, provider name, dates of service, medical record/case number, Medicare/Medicaid ID number, health insurance provider name, health insurance individual policy number, and/or treatment cost.

135. As a result of the Data Breach, Plaintiff Canady made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

136. Plaintiff Canady suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized

disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

137. Plaintiff Canady additionally suffered actual injury when in 2024, unauthorized individuals attempted to open a credit account under her name.

138. Plaintiff Canady additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

139. The Data Breach has caused Plaintiff Canady to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

140. As a result of the Data Breach, Plaintiff Canady anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

141. As a result of the Data Breach, Plaintiff Canady is at a present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

142. Plaintiff Canady has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

**Plaintiff Rachael Reese's Experience**

143. Plaintiff Reese is a patient of Adventist Health Systems in conjunction with health care services she received in Tulare County, California.

144. As a condition of obtaining healthcare services, Plaintiff Reese was required to provide her Private Information to Defendants, including her name, address, date of birth, Social Security number, phone number, and insurance identification number, among other sensitive information.

145. At the time of the Data Breach, Defendants maintained Plaintiff Reese's Private Information in their system.

146. Plaintiff Reese is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Reese would not have entrusted her Private Information to Defendants had she known of Defendants' lax data security policies.

147. Plaintiff Reese received the Notice Letter, by U.S. mail, directly from Defendant Signature, on June 10, 2024. According to the Notice Letter, Plaintiff Reese's Private Information was improperly accessed and obtained by unauthorized third parties, including her address, phone number, date of birth, Social Security number, provider name, dates of service, medical record/case number, Medicare/Medicaid ID number, health insurance provider name, health insurance individual policy number, and/or treatment cost.

148. As a result of the Data Breach, Plaintiff Reese made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

149. Plaintiff Reese suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

150. Plaintiff Reese additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails,

calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

151. The Data Breach has caused Plaintiff Reese to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

152. As a result of the Data Breach, Plaintiff Reese anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

153. As a result of the Data Breach, Plaintiff Reese is at a present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

154. Plaintiff Reese has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

**Plaintiff Lea Jacobs's Experience**

155. Plaintiff Lea Jacobs is, and at all times relevant hereto was, a citizen and resident of the state of North Carolina.

156. Plaintiff Jacobs is a former patient of UNC Health, which, upon information and belief, contracts with Defendant Signature for services.

157. As a condition of receiving healthcare services from UNC Health, Plaintiff Jacobs was required to provide her Private Information, directly or indirectly, to Defendant Signature, including her name, Social Security number, and full health and financial information.

158. At the time of the Data Breach on April 26, 2023, Defendant retained Plaintiff Jacobs's Private Information in its system.

159. Plaintiff Jacobs is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Jacobs would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

160. Plaintiff Jacobs received the Notice Letter, by U.S. mail, directly from Defendant, dated June 10, 2024. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her name and Social Security number.

161. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Jacobs made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, checking her credit monitoring services for fraud, signing up for the service offered and putting a freeze on her credit, changing passwords and logins, and considering whether to change her Social Security number. Plaintiff Jacobs has spent significant time dealing with the Data Breach—at least ten hours thus far—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

162. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from

publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

163. The Data Breach has caused Plaintiff Jacobs to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant have still not fully informed her of key details about the Data Breach's occurrence.

164. As a result of the Data Breach, Plaintiff Jacobs anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

165. As a result of the Data Breach, Plaintiff Jacobs is at a present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

166. Plaintiff Jacobs has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

**Plaintiff Eloyd Long's Experience**

167. Plaintiff Eloyd Long is, and at all times relevant to was, a citizen and resident of the state of California.

168. Plaintiff Long is a former patient at Adventist Health.

169. As a condition of obtaining services at Adventist Health, Plaintiff Long was required to provide his Private Information to Defendants, including his name, social security number, and full health and financial information.

170. At the time of the Data Breach, Defendants retained Plaintiff Long's Private Information in their systems.

171. Plaintiff Long is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Long would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

172. Plaintiff Long received the Notice Letter, by U.S. mail, directly from Defendant, dated June 10, 2024. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his name and Social Security number.

173. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Long made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter and monitoring his financial accounts for any unusual activity, which may take years to detect. Plaintiff Long has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

174. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from

publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

175. The Data Breach has caused Plaintiff Long to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

176. As a result of the Data Breach, Plaintiff Long anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

177. As a result of the Data Breach, Plaintiff Long is at a present risk and will continue to be at increased risk of identity theft and fraud for his lifetime.

178. Plaintiff Long has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

**Plaintiff Monica Enriquez's Experience**

179. Plaintiff Enriquez is a patient of Adventist Health.

180. As a condition of obtaining healthcare services, Plaintiff Enriquez was required to provide her Private Information to Defendants, including her name, address, date of birth, Social Security number, phone number, and insurance identification number, among other sensitive information.

181. At the time of the Data Breach, Defendants maintained Plaintiff's Private Information in their systems.

182. Plaintiff Enriquez is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to Defendants had she known of Defendants' lax data security policies.

183. Plaintiff Enriquez received the Notice Letter, by U.S. mail, directly from Defendant Signature, on June 10, 2024. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her address, phone number, date of birth, Social Security number, provider name, dates of service, medical record/case number, Medicare/Medicaid ID number, health insurance provider name, health insurance individual policy number, and/or treatment cost.

184. As a result of the Data Breach, Plaintiff Enriquez made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

185. Plaintiff Enriquez suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information,

which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

186. Plaintiff Enriquez additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

187. The Data Breach has caused Plaintiff Enriquez to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

188. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

189. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

190. Plaintiff Enriquez has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

**Plaintiff David Underwood's Experience**

191. Plaintiff Underwood is a patient of Adventist Health.

192. As a condition of obtaining healthcare services, Plaintiff Underwood was required to provide his Private Information to Defendants, including his name, address, date of birth, Social Security number, phone number, and insurance identification number, among other sensitive information.

193. At the time of the Data Breach, Defendants maintained Plaintiff's Private Information in their systems.

194. Plaintiff Underwood is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendants had he known of Defendants' lax data security policies.

195. Plaintiff Underwood received the Notice Letter, by U.S. mail, directly from Defendant Signature, on June 10, 2024. According to the Notice Letter, Plaintiffs' Private Information was improperly accessed and obtained by unauthorized third parties, including his address, phone number, date of birth, Social Security number, provider name, dates of service, medical record/case number, Medicare/Medicaid ID number, health insurance provider name, health insurance individual policy number, and/or treatment cost.

196. As a result of the Data Breach, Plaintiff Underwood made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time

Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

197. Plaintiff Underwood suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

198. Plaintiff Underwood additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

199. The Data Breach has caused Plaintiff Underwood to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

200. As a result of the Data Breach, Plaintiff Underwood anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

201. As a result of the Data Breach, Plaintiff Underwood is at a present risk and will continue to be at increased risk of identity theft and fraud for his lifetime.

202. Plaintiff Underwood has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

**Plaintiff Orneze Coit's Experience**

203. Plaintiff Coit is a former patient of UNC Health Southeastern, a client of Signature.

204. As a condition of obtaining healthcare services, Plaintiff Coit was required to provide his Private Information to Defendants, including his name, address, date of birth, Social Security number, phone number, and insurance identification number, among other sensitive information.

205. At the time of the Data Breach, Defendants maintained Plaintiff's Private Information in their system.

206. Plaintiff Coit is very careful about sharing his sensitive Private Information. Plaintiff Coit stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the

internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendants had he known of Defendants' lax data security policies.

207. Plaintiff Coit received the Notice Letter, by U.S. mail, directly from Defendant Signature, on June 10, 2024. According to the Notice Letter, Plaintiffs' Private Information was improperly accessed and obtained by unauthorized third parties, including his address, phone number, date of birth, Social Security number, provider name, dates of service, medical record/case number, Medicare/Medicaid ID number, health insurance provider name, health insurance individual policy number, and/or treatment cost.

208. As a result of the Data Breach, Plaintiff Coit made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach–valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

209. Plaintiff Coit suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized

disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

210. Plaintiff Coit additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

211. The Data Breach has caused Plaintiff Coit to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

212. As a result of the Data Breach, Plaintiff Coit anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

213. As a result of the Data Breach, Plaintiff Coit is at a present risk and will continue to be at increased risk of identity theft and fraud for his lifetime.

214. Plaintiff Coit has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

**All Plaintiffs and Class Members' Experiences**

215. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

216. Plaintiffs and Class Members entrusted their Private Information to Defendants in order to receive Defendants' services.

217. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices.

218. As a direct and proximate result of Defendants' actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

219. Further, and as set forth above, as a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for their lifetimes.

220. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

221. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information,

since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

222. The Private Information maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

223. Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendants. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to Defendants was intended to be used to fund adequate security of Defendants' system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

224. Additionally, Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[17] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[18]

225. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and

[17] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on August 19, 2024).
[18] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on August 19, 2024).

diminished due to their acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

226. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

227. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendants, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of their patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

228. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

## V. CLASS ACTION ALLEGATIONS

229. Plaintiffs bring this action themselves individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

230. Specifically, Plaintiffs propose the following Nationwide Class, subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

231. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs Rachael Reese, Eloyd Long, Monica Enriquez, and David Underwood seek to represent the following subclass:

> **California Subclass**
>
> All individuals residing in California who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

232. The Nationwide Class and California Subclass are collectively referred to herein as the "Class" unless otherwise stated.

233. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which Defendants have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

234. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well as the addition of any state-specific subclasses before the Court determines whether certification is appropriate.

235. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

236. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time,

based on information and belief, the Class consists, at a bare minimum, of 100,000 patients whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendants records, Class Members' records, publication notice, self-identification, and other means.

237. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the FTCA and HIPAA;

c. When Defendants learned of the Data Breach

d. Whether Defendants' response to the Data Breach was adequate;

e. Whether Defendants unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

j. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;

p. Whether Defendants' conduct was negligent;

q. Whether Defendants' conduct was *per se* negligent;

r. Whether Defendants were unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

238. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

239. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

240. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

241. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to

individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

242. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

243. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

## CLAIMS FOR RELIEF

### COUNT I
### NEGLIGENCE
### (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

244. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

245. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

246. Defendants' duty also included a responsibility to implement processes by which it could detect and analyze a breach of their security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

247. Defendants knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Defendants were on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

248. Defendants owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Defendants' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in their possession;

b. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

249. Defendants' duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

250. Defendants' duty also arose because Defendants were bound by industry standards to protect their patients' confidential Private Information.

251. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm.

252. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendants' possession.

253. Defendants, by their actions and/or omissions, breached their duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

254. Defendants, by their actions and/or omissions, breached their duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

255. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that their email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

256. Defendants acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

257. Defendants had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Defendants with their Private Information was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the Private Information stored on them) from attack.

258. Defendants' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

259. As a result of Defendants' ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

260. Defendants' breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

261. As a result of Defendants' negligence in breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their

Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

262. Defendants also have independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

263. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

264. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

265. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

266. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

## COUNT II
## NEGLIGENCE *PER SE*
## (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

267. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

268. Pursuant to Section 5 of the FTCA, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

269. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

270. Specifically, pursuant to HIPAA, Defendants had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

271. Defendants breached their duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

272. Specifically, Defendants breached their duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

273. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect Private Information (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendants duty in this regard.

274. Defendants also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

275. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

276. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and Defendants failure to comply with both constitutes negligence *per se*.

277. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Defendants' negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

278. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

279. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

280. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

**COUNT III**
**BREACH OF IMPLIED CONTRACT**
**(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS AGAINST DEFENDANTS UNC HEALTH AND ADVENTIST)**

281. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

282. This claim is brought on behalf of Plaintiffs and the Nationwide Class against Defendants UNC Health and Adventist (for purposes of this count, "Defendants").

283. Defendants provide healthcare services and medical services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendants regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services and/or entrusting their valuable Private Information to Defendants in exchange for such services.

284. Through Defendants' sale of services to Plaintiffs and Class Members, Defendants knew or should have known that they must protect Plaintiffs' and Class Members' confidential Private Information in accordance with their policies, practices, and applicable law.

285. As consideration, Plaintiffs and Class Members paid money to Defendants and/or turned over valuable Private Information to Defendants. Accordingly, Plaintiffs and Class Members bargained with Defendants to securely maintain and store their Private Information.

286. Defendants accepted payment and/or possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

287. In paying Defendants and/or providing their valuable Private Information to Defendants in exchange for Defendants' services, Plaintiffs and Class Members intended and understood that Defendants would adequately safeguard the Private Information as part of those services.

288. Defendants' implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of their employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

289. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

290. Had Defendants disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Defendants.

291. As providers of healthcare administrative services and medical care, Defendants recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

292. Defendants violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. Defendants further breached these implied contracts by failing to comply with their promise to abide by HIPAA.

293. Additionally, Defendants breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

294. Defendants also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

295. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

296. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

297. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

298. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

299. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforce violations, in violation of 45 CFR 164.306(a)(94).

300. Defendants further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

301. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

302. Defendants further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

303. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide payment and/or accurate and complete Private Information to Defendants in exchange for Defendants' agreement to, *inter alia*, provide services that included protection of their highly sensitive Private Information.

304. Plaintiffs and Class Members have been damaged by Defendants' conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

## COUNT IV
## UNJUST ENRICHMENT
## (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

305. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

306. This Count is pleaded in the alternative to Plaintiffs' breach of implied contract and breach of third-party beneficiary contract claims.

307. Plaintiffs and Class Members conferred a benefit on Defendants by turning over their Private Information to Defendants and by paying for services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

308. Upon information and belief, Defendants funds their data security measures entirely from their general revenue, including from payments made to them by Plaintiffs and Class Members.

309. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

310. Defendants have retained the benefits of their unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

311. Defendants knew that Plaintiffs and Class Members conferred a benefit upon it, which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

312. If Plaintiffs and Class Members had known that Defendants had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendants.

313. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefit of their wrongful conduct.

314. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

315. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by

establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

316. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

## COUNT V
## BREACH OF THIRD-PARTY BENEFICIARY CONTRACT (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS AGAINST DEFENDANT SIGNATURE)

317. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

318. This claim is brought on behalf of Plaintiffs and the Nationwide Class against Defendant Signature (for purposes of this count, "Defendant").

319. Defendant entered into contracts, written or implied, with its clients to perform services that include, but are not limited to, providing healthcare administrative services and medical care. Upon information and belief, these contracts are virtually identical between and among Defendant and their clients around the country whose patients, including Plaintiffs and Class Members, were affected by the Data Breach.

320. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiffs and the Class.

321. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that if it were to breach these contracts with its clients, the clients' patients—Plaintiffs and Class Members—would be harmed.

322. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiffs and Class Members thereof.

323. Plaintiffs and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

324. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

## COUNT VI
## BREACH OF FIDUCIARY DUTY
## (ON BEHALF OF THE PLAINTIFFS AND THE NATIONWIDE CLASS)

325. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

326. In light of the special relationship between Defendants and Plaintiffs and Class Members, whereby Defendants became the guardians of Plaintiffs' and Class Members' Private Information, Defendants became fiduciaries by their undertaking and guardianship of the Private Information to act primarily for Representative Plaintiffs and Class Members, (i) for the safeguarding of Plaintiffs' and Class Members' Private Information, (ii) to timely notify Plaintiffs and Class Members of a data breach and disclosure, and (iii) to maintain complete and accurate records of what information (and where) Defendants did have and continue to store.

327. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship with their customers' patients and former patients—in particular, to keep their Private Information secure.

328. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

329. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

330. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

331. Defendants breached their fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

332. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their Private Information, (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, contest, and recover from identity theft, (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate

measures to protect the Private Information, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, and (vii) the diminished value of Defendants' services they received.

333. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

## COUNT VII
## INVASION OF PRIVACY
## (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

334. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

335. Plaintiffs and Class Members have a legally protected privacy interest in their Private Information, which is and was collected, stored, and maintained by Defendants, and they are entitled to the reasonable and adequate protection of their Private Information against foreseeable unauthorized access and publication of their Private Information to criminal actors, as occurred with the Data Breach. The Private Information of Plaintiffs and Class Members contain intimate details of a highly personal nature, individually and in the aggregate.

336. Plaintiffs and Class Members reasonably expected that Defendants would protect and secure their Private Information from unauthorized parties and that their Private Information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

337. Defendants intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their Private Information to a third party.

338. By failing to keep Plaintiffs' and Class Members' Private Information secure, and disclosing Private Information to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their Private Information obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their Private Information from disclosure to unauthorized persons; and

d. d. enabling the disclosure of their Private Information without consent.

339. This invasion of privacy resulted from Defendants' intentional failure to properly secure and maintain Plaintiffs' and Class Members' Private Information, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

340. Plaintiffs and Class Members' Private Information is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs', and Class Members' Private Information, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

341. The disclosure of Plaintiffs' and Class Members' Private Information to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

342. Defendants' willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and Class Members' intimate and sensitive Private

Information is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

343. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and Class Members' Private Information was without their consent, and in violation of various statutes, regulations and other laws.

344. As a direct and proximate result of Defendants' intrusion upon seclusion, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

**COUNT VIII**
**VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")**
**Cal. Civ. Code § 56, *et seq.***
**(ON BEHALF OF PLAINTIFFS RACHAEL REESE, ELOYD LONG, MONICA ENRIQUEZ, AND DAVID UNDERWOOD AND THE CALIFORNIA SUBCLASS)**

345. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

346. This claim is brought on behalf of Plaintiffs Rachael Reese, Eloyd Long, Monica Enriquez, and David Underwood (for purposes of this count "Plaintiffs") and the California Subclass against Defendants.

347. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

348. Defendant Signature is a "contractor" within the meaning of Civil Code § 56.05(d) within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to

consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Signature, within the meaning of Civil Code § 56.05(k).

349. Plaintiffs and Class Members are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiffs and Class Members fear that disclosure of their medical information could subject them to harassment or abuse.

350. Plaintiffs and Class Members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Signature's computer network at the time of the unauthorized disclosure.

351. Defendants, through inadequate security, allowed unauthorized third-party access to Plaintiffs' and Class Members' medical information, without the prior written authorization of Plaintiffs and Class Members, as required by Civil Code § 56.10 of the CMIA.

352. In violation of Civil Code § 56.10(a), Defendants disclosed Plaintiffs' and Class Members' medical information without first obtaining an authorization. Plaintiffs' and Class Members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendants' violation of Civil Code § 56.10(a).

353. In violation of Civil Code § 56.10(e), Defendants further disclosed Plaintiffs' and Class Members' medical information to persons or entities not engaged in providing direct health care services to Plaintiffs or Class Members, or to their providers of health care or health care service plans or their insurers or self-insured employers.

354. Defendants violated Civil Code § 56.101 of the CMIA through their willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class Members. Defendants' conduct with respect to the disclosure of confidential Private Information was willful and knowing because Defendants designed and implemented the computer network and security practices that gave rise to the unlawful disclosure.

355. In violation of Civil Code § 56.101(a), Defendants created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and Class Members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiffs' and Class Members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendants' violation of Civil Code § 56.101(a). 380. In violation of Civil Code § 56.101(a), Defendants negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and Class Members' medical information. Plaintiffs' and Class Members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendants' violation of Civil Code § 56.101(a).

356. Plaintiffs' and Class Members' medical information that was the subject of the unauthorized disclosure included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

357. In violation of Civil Code § 56.101(b)(1)(A), Defendants' electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiffs' and Class Members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendants' violation of Civil Code § 56.101(b)(1)(A).

358. Defendants violated Civil Code § 56.36 of the CMIA through their failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class Members.

359. As a result of Defendants' above-described conduct, Plaintiffs and Class Members have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36. 385. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the unauthorized disclosure, and violation of the CMIA, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud-risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their Private Information, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their Private Information, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial ac-counts, and mitigating their damages.

360. Plaintiffs, individually and for each member of the Class, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiffs and each Class Member, and attorneys' fees, ligation expenses and court costs, pursuant to Civil Code § 56.35.

**COUNT IX**
**DECLARATORY JUDGMENT**
**(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)**

361. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

362. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

363. Defendants owe a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

364. Defendants still possess Private Information regarding Plaintiffs and Class Members.

365. Plaintiffs alleges that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

366. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure their patients' Private Information and to timely notify customers of a data breach under the common law, HIPAA, and the FTCA;

b. Defendants' existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect patients' Private Information; and

c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

367. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect patients' Private Information, including the following:

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training their security personnel regarding any new or modified procedures;

iv. segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating their patients about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

368. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

369. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

370. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach, thus

preventing future injury to Plaintiffs and other patients whose Private Information would be further compromised.

**COUNT X**
**VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT**
**Cal. Civ. Code § 1798.100 *et seq*.**
**(ON BEHALF OF PLAINTIFFS RACHAEL REESE, ELOYD LONG, MONICA ENRIQUEZ, AND DAVID UNDERWOOD AND THE CALIFORNIA SUBCLASS)**

371. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

372. This claim is brought on behalf of Plaintiffs Rachael Reese, Eloyd Long, Monica Enriquez, and David Underwood and the California Subclass (for purposes of this count "Plaintiffs") and the California Sublcass against Defendants.

373. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
> >
> > (B) Injunctive or declaratory relief.
> >
> > (C) Any other relief the court deems proper.

374. Defendants are a "business" under § 1798.140(b) in that they are corporations organized for profit or financial benefit of their shareholders or other owners, with gross revenue

in excess of $25 million.

375. Plaintiffs and California Subclass Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

376. The Private Information of Plaintiffs and the California Subclass at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the Private Information Defendants collect and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

377. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the California Subclass's Private Information and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information of Plaintiffs and the California Subclass. Specifically, Defendants subjected Plaintiffs and the California Subclass's nonencrypted and nonredacted Private Information to an unauthorized access and exfiltration, theft, or disclosure as a result of

the Defendants' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

378. As a direct and proximate result of Defendants' violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and Class Members' Private Information included exfiltration, theft, or disclosure through Defendants' servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

379. As a direct and proximate result of Defendants' acts, Plaintiffs and the California Subclass were injured and lost money or property, including but not limited to the loss of Plaintiffs' and the Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

380. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." Accordingly, Plaintiff and the California Subclass by way of this complaint seek actual pecuniary damages suffered as a result of Defendants violations described herein. Plaintiff Reese issued a written notice of these alleged violations to Defendants pursuant to § 1798.150(b) on June 18, 2024 and has therefore exhausted all prefiling requirements. The Notice is attached hereto as Exhibit A. Accordingly, Plaintiffs seek statutory damages and injunctive relief pursuant to §1798(a)(1)(A)-(C), (a)(2), and (b).

## COUNT XI
## VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT
## Cal. Civ. Code § 1798.80 *et seq.*
## (ON BEHALF OF PLAINTIFFS RACHAEL REESE, ELOYD LONG, MONICA ENRIQUEZ, AND DAVID UNDERWOOD AND THE CALIFORNIA SUBCLASS)

381. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

382. This claim is brought on behalf of Plaintiffs Rachael Reese, Eloyd Long, Monica Enriquez, and David Underwood (for purposes of this count "Plaintiffs") and the California Sublcass against Defendants.

383. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

384. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

385. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

386. Plaintiffs and members of the California Subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided Private Information to Defendants, directly and/or indirectly, for the purpose of obtaining a service from Defendants.

387. The Private Information of Plaintiffs and the California Subclass at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the Private Information Defendants collect and which was impacted by the cybersecurity attack includes an individual's

first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

388. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the California Subclass's Private Information and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information of Plaintiffs and the California Subclass. Specifically, Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Private Information of Plaintiffs and the California Subclass from unauthorized access, destruction, use, modification, or disclosure. Defendants further subjected Plaintiffs' the California Subclass Members' nonencrypted and nonredacted Private Information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendants' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

389. As a direct and proximate result of Defendants' violation of its duty, the

unauthorized access, destruction, use, modification, or disclosure of the Private Information of Plaintiffs and the California Subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the Private Information of Plaintiffs and the California Subclass by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

390. As a direct and proximate result of Defendants' acts or omissions, Plaintiffs and the California Subclass were injured and lost money or property including, but not limited to, the loss of Plaintiffs' and the Subclass Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses described above. Plaintiffs seek compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

391. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

392. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then

any of the following:

i. the date of the breach,

ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

393. Defendants failed to provide the legally compliant notice under § 1798.82(d) to Plaintiffs and members of the California Subclass. Defendants have violated § 1798.82 by not providing legally compliant and timely notice to Plaintiffs and California Subclass Members. Accordingly, members could have taken action to protect their Private Information, but were unable to do so because they were not timely notified of the breach.

394. On information and belief, many California Subclass Members affected by the

breach, have not received any notice at all from Defendants in violation of Section 1798.82(d).

395. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiffs and California Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

396. As a direct consequence of the actions as identified above, Plaintiffs and California Subclass Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

## COUNT XII
## VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
## Cal. Civ. Code § 1798.80 *et seq.*
## (ON BEHALF OF PLAINTIFFS RACHAEL REESE, ELOYD LONG, MONICA ENRIQUEZ, AND DAVID UNDERWOOD AND THE CALIFORNIA SUBCLASS)

397. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

398. This claim is brought on behalf of Plaintiffs Rachael Reese, Eloyd Long, Monica Enriquez, and David Underwood (for purposes of this count "Plaintiffs") and the California Sublcass against Defendants.

399. Defendants are a "person" defined by Cal. Bus. & Prof. Code § 17201.

400. Defendants violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

401. Defendants' "unfair" acts and practices include:

a. Defendants failed to implement and maintain reasonable security measures to protect Plaintiffs' and California Sublcass Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Defendants failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56);

c. Defendants' failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

402. Defendants have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's

Confidentiality of Medical Information Act (Cal. Civ. Code § 56), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

403. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15

U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and California Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56).

404. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

405. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass Members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

406. Defendants' violations were, and are, willful, deceptive, unfair, and unconscionable.

407. Plaintiffs and California Subclass Members have lost money and property as a result of Defendants' conduct in violation of the UCL, as stated herein and above.

408. By deceptively storing, collecting, and disclosing their Private Information, Defendants have taken money or property form Plaintiffs and California Subclass Members.

409. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and California Subclass Members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

410. Plaintiffs and California Subclass Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs demand a trial by jury on all triable issues.

DATED: September 9, 2024

Respectfully submitted,

*/s/ Bryan L. Bleichner*

Bryan L. Bleichner
Philip J. Krzeski
**CHESTNUT CAMBRONNE PA**
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
*bbleichner@chestnutcambronne.com*
*pkrzeski@chestnutcambronne.com*

Mason A. Barney
Tyler J. Bean
**SIRI & GLIMSTAD LLP**
745 Fifth Avenue, Suite 500
New York, NY 10151
Telephone: (212) 532-1091
Fax: (646) 417-5967
*mbarney@sirillp.com*
*tbean@sirillp.com*

M. Anderson Berry
Gregory Haroutinian
**CLAYEO C. ARNOLD**
**A PROFESSIONAL CORPORATION**
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829
*aberry@justice4you.com*

Jeff Ostrow
**KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT**
One West Law Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 332-4200
*ostrow@kolawyers.com*

***Interim Co-Lead Class Counsel***

Terence R. Coates
**MARKOVITS, STOCK & DEMARCO, LLC**
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651.3700
Fax: (513) 665.0219
*tcoates@msdlegal.com*

Jason M. Wucetich
**WUCETICH & KOROVILAS LLP**
222 North Pacific Coast Highway, Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Fax: (310) 364-5201
*jason@wukolaw.com*

Gary Klinger
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
*gklinger@milberg.com*

Daniel Srourian
**SROURIAN LAW FIRM, P.C.**
3435 Wilshire Blvd. Suite 1710
Los Angeles, CA 90010
Telephone: (213) 474-3800
Fax: (213) 471-4160
*daniel@slfla.com*